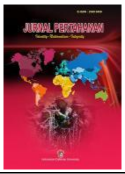

Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 9 No. 2 (2023) pp.350-365
http://jurnal.idu.ac.id/index.php/DefenseJournal

# Implementation of Artificial Intelligence on Indonesia's Defense Intelligence Activities

**Rizky Ramadhianto[1*], Tahan Samuel Lumban Toruan[2], Susaningtyas Nefo Handayani Kertopati[3], Hikmat Zakky Almubaroq[4]**
[1,2,4]Defense Management Study Program, Republic of Indonesia Defense University, Indonesia
[3]Asymmetric Warfare Study Program, Republic of Indonesia Defense University, Indonesia

rizkramdht@gmail.com[1*], tahan.toruan@idu.ac.id[2], susaningtyas@idu.ac.id[3], zakkyauri94@gmail.com[4]
*Corresponding Author

## Article Info

**Article history:**
Received: June 19, 2023
Revised: August 31, 2023
Accepted: August 31, 2023

**Keywords:**
Artificial Intelligence,
Defense Intelligence,
Digital Transformation,
Global Threats,
Intelligence Activities

**DOI:**
http://dx.doi.org/10.33172/jp.v9i2.14657

## Abstract

The global dynamics nowadays are synonymous with technological developments which have led to the concept of digital transformation that needs a more simultaneous and integrated manner. One of them is using Artificial Intelligence technology in defense intelligence activities to prevent sudden strategic attacks on defense forces. Despite of benefits that help intelligence performance in the defense sector, applying Artificial Intelligence technology has potential negative impacts. This article aims to study the significant implications of Artificial Intelligence technology on Indonesia's Defense Intelligence Activities using a qualitative descriptive method in literacy studies originating from journals, books, and credible internet sources. The findings provide that potential threats from Artificial Intelligence-based defense intelligence activities result from both the equipment and capabilities of its users, specifically, they are caused by the processes originating from algorithm miscalculations, data leaks, and statistical errors of defense forces. If the potential threats are not focused on being addressed, it will impact the effectiveness of defense intelligence to reduce uncertainty in forecasting global threats.

## INTRODUCTION

As a result of the dynamics of the global strategic environment, causing a shift in international security patterns towards the implementation of national defense, the characteristics of threats are becoming increasingly complex and multidimensional consisting of military threats, non-military threats, and hybrid threats (Ministry of

Defence of the Republic of Indonesia, 2015). The current challenges and threats to Indonesia's defense and security are no longer in the form of traditional threats that identically use conventional weapons, but have developed into modern and non-traditional threats which are marked by the use of advanced technology in the implementation of national defense.

National defense is essentially all universal defense efforts (Law of the Republic of Indonesia Number 3 of 2002 Concerning National Defense). The state defense doctrine is not dogmatic, but its application is adapted to the development of national interests (Almubaroq, 2020). Thus, the country's defense efforts must also be transformed through technological sophistication to prevent and overcome all forms of digital threats to protect national interests. The development of Indonesia's national interests can be used as a basis when formulating and establishing a grand strategy in the field of national security as well as for creating a national defense system. One of the variables that are determined for the formulation of a defense grand strategy is technology. There is a need for a grand strategy concept to implement the strategies that have been made so that changes in peaceful technology to war technology can materialize if war occurs (Supriyatno, 2014).

The military impact caused by technological developments affects relations between countries, either in the form of creating coalitions and alliances or triggering conflict (Buzan, 2007). Likewise, the war in the era of globalization and digitalization has changed along with technological developments, thus triggering the complexity of emerging threats for implementing Indonesia's defense that come from state actors and non-state actors. The results of the Working Group on Security Sector Reform (2004) confirmed that the developments in defense technology triggered a change in the character of modern warfare, except wars to overthrow the regime, which were no longer dominated by territorial wars carried out with the concepts of guerrilla armed resistance, rather it is a war that emphasizes the destruction of vital infrastructure or the center of gravity. To respond to these global threats, a digital transformation concept is needed in a more simultaneous and integrated manner for the defense process through technology platforms.

The sophistication and modernity of technology in today's non-conventional warfare offer convenience for humans to find ways to carry out the massive proliferation of technology-based weapons at a lower cost, as a result, the resulting impact on the implementation of a country's defense becomes more strategic compared to conventional weapons. An example of technology being developed and applied to prevent sudden strategic attacks on defense forces is digital intelligence technologies on defense intelligence activities. Artificial Intelligence technologies are also being adopted to make better sense of and use intelligence activities, it is particularly good at identifying patterns in reams of data and being used to shift through massive troves of information to provide near real-time intelligence analysis (Wilner, n.d.). With technological advances marked by the use of Artificial Intelligence, it is time to use the potential of these technological advances in intelligence activities to prevent sudden strategic impacts that have a significant impact on Indonesia's national interests.

Artificial Intelligence will transform defense intelligence activities that will have a transformative effect on the strategy of those states employing them. This is because militaries that can successfully develop and utilize them will experience a dramatic increase in fighting power relative to those that cannot (Payne, 2018). In the Indonesian defense domain, there is the Strategic Intelligence Agency (*Badan Intelijen Strategis* or BAIS) entity as an intelligence agency attached to the Indonesian National Armed Forces (TNI) which has the authority to carry out tactical intelligence on intelligence activities in the defense sector based on military and non-military threats. Intelligence is useful in policymaking at the strategic level. Russell (2007) defines intelligence as the knowledge that a country's civilian and military officials must have to maintain prosperity by making warnings of short-term and long-term threats to national interests.

Through the utilization of Artificial Intelligence technologies, the process of sharing intelligence data as well as making decisions and defense policies can be faster, accompanied by empowering human resources that are used less, and capital and operating activities become lighter. However, apart from the conveniences and efficiency obtained, the utilization and development of Artificial Intelligence technologies also have the potential to create various new threats as a result of the consequences they have.

Detection of defense threats in Indonesian defense intelligence activities supported by the use of artificial intelligence technologies should be able to provide optimal benefits in terms of process criteria and results achieved, even though artificial intelligence technology contains various risks behind its use. In a previous artificial intelligence study, Moran, Burton, & Christou (2023) explain that the US Intelligence Community (IC) that uses Artificial Intelligence can improve the intelligence cycle and diminish clandestine operations, eventually reducing surveillance costs. But at the same time, it can be a potential consequence in the form of tech sector companies that are involved with many diverse constituencies, so it is hard to reach belief systems. In the context of Indonesia, there is a tendency not to relate many aspects of Artificial Intelligence research to defense intelligence activities, as a result, the findings in this research will open up horizons and add new insights. This study aims to discuss the potential consequences of using Artificial Intelligence in various defense intelligence activities conducted by Indonesia using a qualitative descriptive method in the form of a literature review.

## METHODS

This study uses a qualitative method with a descriptive analysis approach. According to Strauss and Corbin, qualitative research is research that can be used to examine people's lives, history, behavior, and function of organizations, social movements, or kinship relationships that produce discoveries that cannot be achieved using statistical procedures or quantitative methods (Nugrahani, 2014). The research focuses on qualitative and researched methods to see the extent of the challenges caused by the application of Artificial Intelligence technologies for defense intelligence activities.

The qualitative approach was chosen by the researcher through detailed data collection from information sources. The data obtained came from sources related to the object of the literature review. This method is adopted to find a broad view of various information relevant to the object under study through published data such as international organizations' publications, journals, books, scholars, and university reports, as well as official documents related to the implementation of artificial intelligence technology in intelligence activities along with its implications in the context of supporting national defense.

A study by Ayoub & Payne (2015) indicates that Artificial Intelligence will be useful at both tactical and strategic levels, which strive to be free from destructive hazards by providing security guarantees for their users. Data related to the two components, namely artificial intelligence and defense intelligence namely BAIS TNI were explored at an early stage through studies of various literacies. It is a data collection technique derived from public documents, such as official reports, private documents, journals, and books (Creswell, 2014). In the next stage, the data that has been collected is combined with data related to the implementation of the two research components that have been carried out in several countries. At the end of the stage, there is a study of the implications of the two components when implemented in the Indonesian defense system.

## RESULT AND DISCUSSION

### Artificial Intelligence

The emergence of Artificial Intelligence technology in the mid-1950s was initiated by John McCarthy who explained it comprehensively as the 'science and engineering of making intelligent machines' (Teneo.ai, n.d.). Understanding of the meaning of Artificial Intelligence for each person varies based on the background and profession that person is engaged in, so there is a vast gap between the reality of what Artificial Intelligence can do and the understanding, expectations, and fears of the public, including often informed policymakers (Boulanin, 2019). Based on its use, Conn (2015) categorizes Artificial Intelligence technology into two systems, namely narrow/weak Artificial Intelligence and general/strong Artificial Intelligence often referred to as Artificial General Intelligence (AGI).

Technological and scientific progress, especially the rapid development of information technology, plays a crucial role in peace and security issues (Reuter, 2019). One of them is the utilization of Artificial Intelligence as a sub-discipline of computer science, dealing with computer systems capable of performing tasks that require human intelligence (Kersting, 2018). The basic principle of implementing AI technologies must be based on the benefit and goodness of people by the applicable code of ethics. These codes of ethics focus on the transparent, ethical, and accountable use of Artificial Intelligence technologies such as human agency and oversight which indicate that humans can operate Artificial Intelligence technologies wherever and whenever they need (Mikalef, Conboy, Lundström, & Popovič, 2022).

Reflecting on history, research to develop Artificial Intelligence technology began in 1950 when Alan Turing attempted to answer the question of whether machines can think (Epstein, Roberts, & Beber, 2008). Although there are several different perspectives in classifying the phases of Artificial Intelligence technology development, Russel & Norvig (2009) strictly divide them into phases: the gestation of Artificial Intelligence (1943-1955), the birth of Artificial Intelligence (1956), early enthusiasm, great expectations (1952-1969), a dose of reality (1966-1973), knowledge-based systems: the key to power? (1969-1979), Artificial Intelligence becomes an industry (1980-present), the return of neural networks (1986-present), Artificial Intelligence adopts the scientific method (1987-present), the emergence of intelligent agents (1995-present), and the availability of very large data sets (2001-present).

In the development of Artificial Intelligence technology, algorithms dominate the focus echoed by experts in their studies. However, this is different from Yarowsky and Efros on Ahmad (2018) who stated that there are more important studies than algorithms to induce cognition and intelligence into a machine's behavior, it is large data. This means that the large data can be applied to the spectrum of the Artificial Intelligence power systems as a whole with a wider scope by categorizing various conflicts from the smallest to the largest scale, from the lowest intensity to the highest. This indication is directly proportional and positively correlated to the algorithm entity as the main focus on Artificial Intelligence so far which has faded due to the discovery of the large data.

**Table 1.** Artificial Intelligence Domains (Lahmann, Keiser, & Stierli (2018)

| Domain | Description |
|---|---|
| Algorithmic Game Theory and Computational Social | Systems that address the economic and social computational dimensions of Artificial Intelligence, such as how the system can handle potentially misaligned incentives, including humans, companies, and automated Artificial Intelligence-based agents that represent them. |
| Natural Language Processing (NLP) | An algorithm that processes human language input and then converts it into an understandable representation. |
| Computer Vision (Visual Analysis) | The process of extracting relevant information from an image or images for further classification and analysis. |
| Machine Learning | Learning algorithm design, as well as scaling existing algorithms, to work with large data sets. |
| Deep Learning | The model consists of inputs such as images or audio and some hidden layers of sub-models. These serve as inputs for the next layer and are ultimately the output of the activation function. |
| Soft Robotics (Robotic Process Automation) | Automate repetitive tasks and common processes such as customer service and sales without the need to modify existing Information and Technology system maps. |
| Collaboration System | Models and algorithms help develop autonomous systems that can work collaboratively with other systems as well as humans. |

According to Johnson (2021), it is easy to overstate the opportunities and challenges posed by the development and deployment of Artificial Intelligence in the military sphere. Artificial Intelligence technology in the aspect of defense can be operated in several dimensions to create algorithms on drone platforms for surveillance functions, directing physical objects such as robotic systems, and acting without human supervision. As a result, these functions can reduce dependence on the number of troops deployed on tanks, aircraft, and ships (Ryan, 2017). Artificial Intelligence will play a more role in the tactical domain. It is a consideration of the possibility of more ambiguity arising to make decisions and reward functions that any machine seeks to satisfy from the strategic domain, however, this does not diminish the importance of decision-making at the strategic level.

Another thing was stated by Allen & Chan (2017) that Artificial Intelligence can help process and interpret information. An example is the image recognition algorithm used for the identification process in a US military project called Maven, in which this program seeks to develop algorithms to automate the process of analyzing video feeds captured by drones. Artificial Intelligence systems with overlapping characteristics can be used as new forms of command and control in the form of operational systems, including battle management to analyze large data sets and make predictions to direct actions based on algorithms (Roff, 2018).

Then there are the unique concerns about the capacity of Artificial Intelligence technologies to deal with ambiguous and rapidly evolving data and to learn from limited data; his ability to understand complex associative meanings and develop imaginative responses; and its capacity to effectively interpret and carry out the human intentions that support its activities, even where these are complex and multifaceted in themselves. A similar thought was expressed by Levine, Lillicrap, & Kalakrishnan (2016) regarding intelligence agents and analysts learning from previous actions or by observing the parallel actions of other agents in their network through Artificial Intelligence-based devices, which are both proficient and can be confusing in making conclusions based on data on the battlefield.

Ernest et al. (2016) argue that autonomous platforms based on Artificial Intelligence will be able to maneuver faster by using more precise forces than those operated by humans. An example that has been implemented is an Artificial Intelligence system that can outperform experienced military pilots in simulated air-to-air combat. In the context of the Indonesian defense system, if it utilizes and develops Artificial Intelligence technology, it will experience a dramatic increase in combat power. This is based on the characteristics of the technology that will transform defense activities such as intelligence and surveillance, logistics, and weapons design simultaneously, from being tactical to having a strategic effect.

Mikalef et al. (2022) recommend Artificial Intelligence operators be open about the reasons for using and the weaknesses of Artificial Intelligence in the various activity processes that will be carried out. This is for the sake of creating transparency that can be accessed by stakeholders through real documentation, to be able to build an understanding among people regarding the system's behaviors while upholding privacy to emphasize the security of data and lawful data collection.

Furthermore, he emphasized that in its implementation, it is undeniable that there is the possibility of errors and mistakes produced by Artificial Intelligence systems. Therefore, it is important to prioritize the principle of accountability for operators in every action they take to prevent any irresponsible actions through a humane approach to create Artificial Intelligence systems that are inclusive by involving various communities. So that diversity and a system of non-discrimination will be created for all elements of society, where the use of Artificial Intelligence can be more beneficial for all groups, from the majority to a minority group.

**Defense Intelligence**

Along with the development of an increasingly sophisticated world, it also has an impact on techniques in intelligence science which are also developing following directions, and adapting to the dynamics that occur. Intelligence can be interpreted as the ability to think or analyze humans to understand the nature of various security threats and anticipate them with the main task of detection and early warning. Intelligence also means the art of finding, collecting, and processing strategic information needed by a country about "enemy" countries (Hendropriyono, 2014). Collins & Kingston (2001) describe a series of activities in target intelligence to be able to answer questions such as: based on the enemy's defensive strength, what actions should be taken to overcome them; based on estimates of past motives, opportunities, weaknesses, obstacles, and precedents, what kind of military action the enemy might take; and also based on a certain scale and comparison of related defenses, what kind of defense is the enemy's most potential countermeasures.

In general, intelligence is understood into four meanings, namely intelligence as information, process, series of missions, and organization (Johnson, 1998). In principle, intelligence activities have two main actions, namely collecting and analyzing. These two things must be seen from a broader perspective, to relate these activities to the needs of decision-makers and the use of finished intelligence products. This is done through the concept of the intelligence cycle, which is a process of obtaining the information, then converting it into intelligence products and presenting it to the stakeholders.

Kautilya in Prabhu & Dwivedi (2015) spoke about the vital role of intelligence in national defense which consists of early detection to find out the possibility of irregularities in something that could arise as a threat; an early warning that aims to prevent the public and prevent the emergence of threats to many people and the country from various threats. Intelligence must facilitate the continued achievement of long-term goals while also guiding rational tactical choices to respond to external developments. Intelligence has a contribution function to the processes, products, and organizations used by senior officials to make and implement national policies and national defense.

Scott & Jackson (2004) further explain that in carrying out each of its activities, intelligence does not escape failure in anticipating threats that can be caused by several factors, such as the inability of intelligence officers to carry out their role in an unfamiliar environment, failure to organize and coordinate information and analysis of information originating from various intelligence services, limited resources to collect, translate and analyze information, failure of political leaders to understand the meaning and limitations of intelligence, politicization (engineering) of intelligence products to suit the wishes of political leaders. The analysis is carried out based on belief in something that appears to be if it's true (wishful thinking as self-delusion), ego-centric, and cooperative relations that don't go well between intelligence officers and policymakers.

Concerning defense, the defense intelligence entity is a combination of intelligence forces and the armed forces under the coordination of the Ministry of Defense which has been in existence since the 1960s. De Graaff & Nyce (2016) gave examples of intelligence agencies working in the defense sector in several countries, such as the Defense Intelligence (DI) in England, the Directorate of Military Intelligence (DMI) in France, the Defense Intelligence Agency (DIA) in the United States, and The Netherlands Defence Intelligence and Security (NLD DISS) has a similar objective to that stated by Davies (2016) regarding the designation of defense intelligence for political and command staff levels. Therefore it can be identified through the strategic level of military doctrine, to decision-making and policies in supporting the implementation of defense comprehensively.

Davies (2016) explains if the unique character that comes from the military domain, defense intelligence has a different approach from intelligence in general both conceptually and practically in responding to a conventional problem. This argument is in line with the thinking of Herman (1996) who previously considered that the position of defense intelligence is often more central than it should be. Luttwak (2002) classifies intelligence in the defense and military environment into strategic intelligence and tactical intelligence based on the level of strategy from the highest to the lowest: grand strategy, theater level of strategy, operational level of strategy, tactical level of strategy, and technical level of strategy.

Defense intelligence has different characteristics based on the results of several intelligence and military literacy studies. The first feature is the existence of defense intelligence inherent in the military organization, encompassing the relationship between defense intelligence, agencies, and military decision-makers and the relationship between them and the branches of the intelligence services responsible for intelligence gathering, analysis, and dissemination during military missions.

Rietjens (2020) revealed that the involvement of this organization creates a more intimate relationship with clients who are the most important in defense intelligence, therefore it is only natural that it has the potential to generate stronger pressure compared to civilian intelligence in terms of assessing the interests of defense organizations. An example is in the case of military deployment, where there is an adjustment of confidence and a decrease in the level of threat to garner the support of a parliamentary majority. Defense intelligence differs from civilian intelligence in terms of support with the characteristic of irrelevance to a political threat, this is because the purpose of intelligence support at all levels under the auspices of the Ministry of Defense and lower tactical levels such as mission support is solely to support policies that ongoing.

The second characteristic of defense intelligence is the membership composition which is a combination of military and civilian personnel. Defense intelligence has a unique dual position because it is in the middle of a dichotomy between military and civilian intelligence cultures (Thomson, 2015). This blend brings together specific issues of shared identity, different approaches to leadership styles, optimal use of different backgrounds, and different career and training opportunities (North Atlantic Treaty Organization Science and Technology Organization HFM-226 Task Group, 2018; Goldenberg et al., 2019). The result is conflicting interests between military and civilian personnel in the context of intelligence producer and client relations.

The third characteristic is the distinctive culture of the military organization which also influences the characteristics of defense intelligence, including the existence of a strong hierarchy. In military organizations, hierarchies have a strong position and influence on the running of the organization when compared to non-military agencies. This is considered a method of training discipline and order (Holmberg & Alvinius, 2019). Herman (1996) argues that the assertive nature and work of military teams may conflict with the need for an intelligence qualification that is full of shades of gray.

In terms of functions and authorities, there may be an overlap between strategic defense intelligence and military intelligence, which structurally decreases from the strategic level to the operational and tactical levels. An example of this overlap is found in the Defense Intelligence Agency which generally handles the national level as well as long-term and strategic intelligence needs, but at the same time is designated as a combat support agency (Zohar, 2015). This can lead to miscoordination where one of the driving factors is technological developments which make it increasingly possible for military intelligence support to carry out missions outside the scope and area of the mission (Ministerie van Defensie, 2012). Operational and tactical activities can be undertaken by defense intelligence to engage actively in intelligence support beyond the strategic level. This can also have implications for the concerns of defense intelligence analysts in compiling reports that deviate from their responsibility to analyze operational or tactical threats to become more strategic. Based on this, it appears that strategic compression adds to the complexity of the defense intelligence structure.

When talking about Indonesian defense intelligence, since the military and defense were separated based on the results of the reform, the Ministry of Defence of the Republic of Indonesia no longer has an organization that provides the necessary defense intelligence. The Ministry of Defence of the Republic of Indonesia has the task of carrying out government affairs in the field of defense, in the implementation stage of its duties, one of the aspects needed is defense intelligence which has projections for designing defense strategies. Defense Intelligence is included in one of the scopes of State Intelligence which in the Law on State Intelligence is administered by the Strategic Intelligence Agency (BAIS) of the Indonesian National Armed Forces (TNI). The position of BAIS TNI is more at the operational level which provides strategic analysis for use in the context of the operational interests of the TNI. The purpose of the existence of BAIS TNI is to carry out intelligence activities attached to the Indonesian National Armed Forces which has the authority to carry out intelligence activities in the defense sector based on military and non-military threats. BAIS TNI makes full use of intelligence as an activity in obtaining information about Indonesian defense.

## Analysis of Implementation

The implementation of defense is based on awareness of the rights and obligations of citizens, as stated in the national goals based on the Constitution of the Republic of Indonesia Paragraph 4 of 1945, namely to protect the Indonesian nation and all of Indonesia's bloodshed, and to promote the general welfare, educate the nation's life, and participate in carrying out the burdens of the world based on freedom, eternal peace, and social justice. For intelligence agencies tasked with defense by identifying a large collection of data and information patterns, the use and development of weapons technology is a necessity. Artificial Intelligence is very useful for defense intelligence activities because of the large data sets available for analysis, so it is directly proportional to the ability to collect intelligence information as a result of advances in Artificial Intelligence technology.

In the autonomous decision-making process by networked computer agents, the Artificial Intelligence system contributes specifically to enable very fast sequential actions in various places and conditions, even in uncertain intelligence operating environments. In the current era, Artificial Intelligence technology is indeed reliable according to the field of expertise, but it lacks innovation by switching to other types of tasks. Nonetheless, the rapid progress achieved in Artificial Intelligence research, especially through the mechanism of a hybrid approach which is characterized by the use of several techniques at its disposal, shows the potential for Artificial Intelligence technology to significantly influence existing defense activities in the short to medium term. This is in line with the stronger ability of the hardware attached to it in processing algorithm commands.

There are several things have been raised which are intended for the defense sector, especially the military. First, Artificial Intelligence will change the balance of power where the effectiveness of Artificial Intelligence is projected to be able to outperform old military capabilities, thereby dramatically changing the balance of power. This will change the usability of forces by reducing risks for operators in utilizing Artificial Intelligence combat systems. Its utilization will no doubt be able to increase its military capabilities to scout, maneuver, and use deception before concentrating power quickly and firing precision shots. Moreover, marginal technological advantages in Artificial Intelligence tend to have a disproportionate effect on the battlefield considering small advantages in decision-making ability, especially in terms of speed and accuracy, which can translate disproportionately into dominance.

Second, the use of Artificial Intelligence can reduce the risk of using violence, especially for countries that aim to avoid as few victims as possible but still have a great chance of dealing with this potential for violence. Changes in payment systems linked to fighting could trigger conflict in countries that had avoided the risk of violence until recently. Uniquely, in other places, Artificial Intelligence can prevent the aggression of adventurers who are no longer under the threshold of intervention in seeking easy profits.

Third, there is a difference between nuclear weapons systems and Artificial Intelligence systems used by the military in defense. If nuclear weapons can survive the first strike, Artificial Intelligence has the potential to change the balance. This means that Artificial Intelligence is oriented towards activities that support attacks, record speed, and accuracy, and acquire and analyze unbiased knowledge and data.

Fourth, Artificial Intelligence will comprehensively shape military activities across the spectrum of violence, instead of maintaining clear normative differences between conventional and unconventional systems that develop in the case of nuclear weapons. This is because utility levels range from the smallest to the most massive, enabling a nation to dominate escalation against conventionally equipped adversaries of any intensity and for any type of hostilities. As a result, it creates disparities where certain countries can enjoy a comparative advantage over rival countries, but this does not apply to countries that do not have a comparative advantage.

One of the Artificial Intelligence technologies, namely Machine Learning, can be utilized in collection, processing, and analysis activities such as speech-to-text transcription, including identifying human speech in noisy environments and cross-language translation which is half of the Intelligence Cycle. Even so, its utilization will be less than optimal in intelligence planning, dissemination, and evaluation activities. Therefore, the implementation of Artificial Intelligence technology in Defense Intelligence apart from receiving and processing defense information should also be able to determine what information will be retrieved (planning), help communicate information (dissemination), and help compare risks and business usefulness (evaluation). On the other hand, the technology is considered less competent to prioritize the most important intelligence gathering, where the output of Machine Learning algorithms applied to raw intelligence data is better considered as the foundation of intelligence, not the final analysis.

In intelligence activities, there is the prospective value from Artificial Intelligence in the form of Deep Learning, a term that refers to Machine Learning techniques of multi-layer neural networks. Deep Learning excels in "activities consisting of input-output vector mapping," as stated in the book Deep Learning by Goodfellow, Bengio, & Courville (2016) from Apple also Yoshua Bengio and Aaron Courville who are the University of Montreal, professors. Deep Learning tools have made tremendous advances in areas such as image recognition for objects, speech recognition, and language translation, and the acceleration of processing raw intelligence data is also not without their limitations. As a result, caution is needed to detect unexpected events by considering that intelligence activities often deal with these situations.

Artificial Intelligence can assist defense intelligence in determining the truth and reducing uncertainty, but it can also have the opposite effect caused by the consequences of using Artificial Intelligence technology itself. Strategies to counteract and understand the development of threats to the use of Artificial Intelligence in the defense sector can be implemented by strengthening defense intelligence capabilities through Artificial Intelligence technology devices as well.

In essence, Artificial Intelligence technologies require security from the process of sharing data between devices, especially data that is both sensitive and strategic. Data that is sent or on the server can be leaked, it can be misused by irresponsible parties which can result in loss of privacy from sensitive and confidential data. If secret data is leaked, this is contrary to the intelligence information system which prioritizes the principle of confidentiality. Some efforts can be taken by using well-encrypted data and using strict procedures for sharing data and storing it. Moreover, the data must also be equipped with security procedures from attempts to steal and break data, which in the future will be more prevalent.

Another thing that can be caused by Artificial Intelligence with its fast-processing character is increasing the potential for failure to organize and coordinate information analysis from the defense intelligence service. The ability to process information faster by Artificial Intelligence has an impact on reducing the level of dependence on defense intelligence human resources, as a result, negligence in organizing and coordinating intelligence information is unavoidable due to the lack of supervision.

Large data sets related to defense systems in Artificial Intelligence processing can also be a problem for intelligence capabilities to understand the associative meaning of statistical information which is increasingly complex as a result of the application of the technology. It surely can result in the interpretative ambiguity of defense intelligence data which is limited in nature, so transparency and accountability are required in every activity. However, if these two principles are published to the general public, they will conflict with the principle of intelligence secrecy.

Utilization and development of Artificial Intelligence tools can lead to miscoordination, for example in the form of processing intelligence reports that deviate from what was originally targeted. This will also be exacerbated based on the characteristics of intelligence, especially in the defense sector, which tends to prioritize hierarchies that cause strong pressure from several internal parties, and ego-centrist attitudes among intelligence personnel, resulting in conflicting interests. As a result, it will have an impact on the position and a strong influence on the way the organization operates Artificial Intelligence devices.

In the end, the potential threat from Artificial Intelligence-based defense intelligence activities that have been described previously can create failures in answering various questions about the defense forces of other countries. These failures include miscalculation of the algorithmic process in the intelligence data collection phase, breaches in the process of sharing strategic defense data, and errors in processing statistical data as an effort to observe the reactions of other countries to maintain a balance of defense forces, resulting in misinterpretation of estimating other countries power along with their intentions in deploying military force.

## CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

The use of Artificial Intelligence technologies in defense intelligence activities can contain positive values as well as negative meanings which are not only caused by technical influences originating from the equipment but also from the capabilities of its users. Defense intelligence activities that should run smoothly to anticipate sudden strategic actions by other countries against Indonesia's national interests can become vulnerable to emerging threats due to algorithm miscalculations, data leaks, and statistical errors of defense forces based on the results of Artificial Intelligence processing.

Even though the potential negative impact of using Artificial Intelligence technologies on defense intelligence activities can be anticipated as early as possible, in the future, there are still many potential threats based on them that will reduce the effectiveness of defense intelligence. So proper planning is needed in the development of the Artificial Intelligence system in the process of defense intelligence activities to reduce uncertainty in forecasting global threats. In the future, it is hoped that a study will be carried out that focuses more on the comparison of the use of Artificial Intelligence technologies for intelligence activities by countries in the region so that new methods can be found to respond to negative issues as well as to build potential for collaboration in the development of the technology.

This research has several limitations in the data collection process, where the data collected came from literature studies. To overcome this, further research that has a relevant focus is required to collect data from credible informants who are directly involved with the object of research through categorization techniques starting from key, main, to supporting informants.

## REFERENCES

Ahmad, K. (2018). Artificial Intelligence and the Changing Nature of Warfare. *Stratagem: Journal of the Centre for Strategic and Contemporary Research*, *1*(2), 57–72. https://journal.cscr.pk/stratagem/index.php/stratagem/article/view/26

Allen, G., & Chan, T. (2017). *Artificial Intelligence and National Security*. Cambridge: Belfer Center for Science and International Affairs Harvard Kennedy School.

Almubaroq, H. Z. (2020). *Bahan Ajar Strategi Pertahanan*. Bandung: Indonesia Emas Group.

Ayoub, K., & Payne, K. (2015). Strategy in the Age of Artificial Intelligence. *The Journal of Strategic Studies*, *39*(5), 793–819. https://doi.org/10.1080/01402390.2015.1088838

Boulanin, V. (2019). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*. Sweden: Stockholm International Peace Research Institute.

Buzan, B. (2007). *People, States & Fear: an Agenda for International Security Studies in the Post-Cold War Period: an Agenda for International Security Studies in the Post-Cold War Era*. United Kingdom: ECPR Press.

Collins, J. M., & Kingston, R. C. (2001). *Military Strategy: Principles, Practices, and Historical Perspectives*. United States: Potomac Books, Inc.

Conn, A. (2015, November 14). Benefits & Risks of Artificial Intelligence. Retrieved July 31, 2023, from https://futureoflife.org/ai/benefits-risks-of-artificial-intelligence/?cn_reloaded=1

Cresswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. Washington DC: SAGE Publications.

Davies, P. H. J. (2016). The Problem of Defence Intelligence. *Intelligence & National Security*, *31*(6), 1–13. https://doi.org/10.1080/02684527.2015.1115234

De Graaff, B., & Nyce, J. M. (2016). *Handbook of European Intelligence Cultures*. United Kingdom: Rowman & Littlefield.

Epstein, R., Roberts, G., & Beber, G. (2008). *Parsing the Turing Test: Philosophical and Methodological Issues in the Quest for the Thinking Computer*. Berlin: Spinger.

Ernest, N., Carroll, D., Schumacher, C., Clark, M., Cohen, K., & Lee, G. (2016). Genetic Fuzzy based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions. *Journal of Defense Management*, *6*(1). https://www.researchgate.net/publication/301944635_Genetic_Fuzzy_based_Artificial_Intelligence_for_Unmanned_Combat_Aerial_Vehicle_Control_in_Simulated_Air_Combat_Missions

Goldenberg, I., Andres, M., Osterberg, J., James-Yates, S., Johansson, E., & Pearce, S. (2019). Integrated Defence Workforces: Challenges and Enablers of Military-Civilian Personnel Collaboration. *Journal Military Study*, *8*, 28–45. https://doi.org/10.2478/jms-2019-0004

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning (Adaptive Computation and Machine Learning series)*. Cambridge: The MIT Press.

Hendropriyono, A. M. (2014). *Filsafat Intelijen Negara Republik Indonesia*. Jakarta: Kompas.

Herman, M. (1996). *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Holmberg, A., & Alvinius, A. (2019). How Pressure for Change Challenge Military Organizational Characteristics. *Defence Studies*, *19*(2), 130–148. https://doi.org/10.1080/14702436.2019.1575698

Johnson, J. (2021). *Artificial Intelligence and The Future of Warfare: The USA China and Strategic Stability*. Manchester: Manchester University Press.

Johnson, L. K. (1998). *SecretAagencies: U.S. Intelligence in a Hostile World*. London: Yale University Press.

Kersting, K. (2018). Machine Learning and Artificial Intelligence: Two Fellow Travelers on the Quest for Intelligent Behavior in Machines. *Specialty Grand Challenge*, *1*, 1–4. https://doi.org/10.3389/fdata.2018.00006

Lahmann, M., Keiser, P., & Stierli, A. (2018). *AI will transform project management. Are you ready?* Switzerland: PwC Switzerland.

Law of the Republic of Indonesia Number 3 of 2002 concerning National Defense.

Levine, S., Lillicrap, T., & Kalakrishnan, M. (2016). How Robots Can Acquire New Skills from Their Shared Experience. Google Research Blog. Retrieved July 31, 2023, from https://research.googleblog.com/2016/10/how-robotscan-acquire-new-skills-from.html

Luttwak, E. N. (2002). *Strategy: The Logic of War and Peace*. Cambridge: Harvard University Press.

Mikalef, P., Conboy, K., Lundström, J. E., & Popovič, A. (2022). Thinking Responsibly about Responsible AI and 'the Dark Side' of AI. *European Journal of Information Systems*, *31*(3), 257–268. https://doi.org/10.1080/0960085x.2022.2026621

Ministerie van Defensie. (2012). *Joint Doctrine Publicatie 2 Inlichtingen*. Den Haag: Ministerie van Defensie.

Ministry of Defence of the Republic of Indonesia. (2015). *Buku Putih Pertahanan*. Jakarta: Ministry of Defence of the Republic of Indonesia.

Moran, C. R., Burton, J., & Christou, G. (2023). The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, *8*(2). https://doi.org/https://doi.org/10.1093/jogss/ogad005

North Atlantic Treaty Organization Science and Technology Organization HFM-226 Task Group. (2018). *Civilian and Military Personnel Integration and Collaboration in Defence Organisations*.

Nugrahani, F. (2014). *Metode Penelitian Kualitatif*. Solo: Cakra Books.

Payne, K. (2018). Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*, *60*(5), 7–32. https://doi.org/10.1080/00396338.2018.1518374

Prabhu, V., & Dwivedi, L. D. (2015). Kautilya's Views on Espionage and its Current Relevance. *International Knowledge Sharing Platform*, *5*(7), 64. https://www.iiste.org/Journals/index.php/RHSS/article/view/21517

Reuter, C. (2019). *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Berlin: Spinger.

Rietjens, S. (2020). Intelligence in Defence Organizations: a Tour de Force. *Intelligence & National Security*, *35*(5). https://doi.org/10.1080/02684527.2020.1737397

Roff, H. M. (2018, May 10). COMPASS: a New AI-Driven Situational Awareness Tool for the Pentagon? Retrieved July 31, 2023, from https://thebulletin.org/2018/05/compass-a-new-ai-driven-situational-awareness-tool-for-the-pentagon/

Russel, S., & Norvig, P. (2009). Artificial Intelligence: a Modern Approach. In *The Knowledge Engineering Review*. London: Pearson. https://doi.org/10.1017/S0269888900007724

Russell, R. L. (2007). Sharpening Strategic Intelligence: Why the CIA Gets it Wrong, and What Needs to be Done to Get it Right. In *Sharpening Strategic Intelligence: Why the CIA gets it Wrong, and What Needs to be Done to get it Right*. Cambridge: Cambridge University Press. https://doi.org/10.1017/cbo9780511509902

Ryan, M. (2017, December 11). Building a Future: Integrated Human-Machine Military Organization. Retrieved July 31, 2023, from https://thestrategybridge.org/the-bridge/2017/12/11/building-a-future-integrated-human-machine-military-organization

Scott, L. V., & Jackson, P. (2004). *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*. United Kingdom: Routledge.

Supriyatno, M. (2014). *Tentang Ilmu Pertahanan*. Jakarta: Yayasan Pustaka Obor Indonesia.

Teneo.ai. (n.d.). Homage to John McCarthy, the Father of Artificial Intelligence (AI). Retrieved July 31, 2023, from https://www.teneo.ai/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence-ai

The Constitution of the Republic of Indonesia Paragraph 4 of 1945.

Thomson, J. (2015). Governance Costs and Defence Intelligence Provision in the UK: A Case-Study in Microeconomic Theory. *Intelligence & National Security*, *31*(6). https://doi.org/10.1080/02684527.2015.1115239

Wilner, A. S. (n.d.). *Artificial Intelligence and Deterrence: Science, Theory and Practice*. https://www.sto.nato.int/publications/sto%20meeting%20proceedings/sto-mp-sas-141/mp-sas-141-14.pdf

Working Group on Security Sector Reform. (2004). *Monograph No-3: Kaji Ulang Strategi Pertahanan Nasional*. ProPatria.

Zohar, E. (2015). Israeli Military Intelligence’s Understanding of the Security Environment in Light of the Arab Awakening. *Defence Studies*, *15*(3), 203–234. https://doi.org/10.1080/14702436.2015.1065612